IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
FAYETTEVILLE DIVISION

UNITED STATES OF AMERICA **PLAINTIFF**

V. **Case No. 5:15-CR-50087-001**

ANTHONY ALLEN JEAN **DEFENDANT**

***** UNDER SEAL *****

MEMORANDUM OPINION AND ORDER

Now pending before the Court is Defendant Anthony Allen Jean's Motion to Compel (Doc. 28) and supporting expert-witness declarations, filed on June 10, 2016. The Government filed an under-seal Response in Opposition to the Motion (Doc. 30) on June 21, 2016. The Government's Response was also supported by expert declarations, as well as certain emails and letters that the parties had exchanged regarding this discovery dispute. The parties previously entered into an agreed Protective Order (Doc. 26) regarding the handling of certain material the Government had deemed confidential, and this discovery dispute arose after the Protective Order was in place.

Prior to filing the Motion to Compel, Mr. Jean had filed a Motion to Suppress (Doc. 19) on March 21, 2016. The Court elected to take up the suppression issue first, holding an evidentiary hearing on June 23, 2016. The Motion to Suppress was denied in a Memorandum Opinion and Order (Doc. 40) filed on September 13, 2016. The Court then scheduled an evidentiary hearing on the Motion to Compel, and invited the parties to submit supplementary briefing if they so desired, particularly if their positions had changed in the intervening months due to new evidence produced by the Government, or due to

new case law impacting any of the issues raised in the Motion. Mr. Jean declined to file a supplementary brief and informed the Court that the Government had not surrendered any new evidence. The Government filed a Supplemental Response to the Motion to Compel (Doc. 41), pointing the Court to two opinions from the Eastern District of Virginia, regarding similar discovery issues arising from the same FBI sting operation that led to Mr. Jean's arrest.

The Court held an evidentiary hearing on the Motion to Compel on October 11, 2016, and Mr. Jean called expert witness Dr. Matthew Miller to testify via videoconference, while the Government called expert witness Special Agent Daniel Alfin to testify in person. Both witnesses were subject to cross-examination by counsel, and the Court made its own inquiries of the witnesses, as well. Both sides were also given the opportunity to present oral argument to the Court at the close of the hearing. The Court took the matter under advisement, stating that it would first endeavor to decide the issue of whether the requested discovery was material to the defense, and then, if necessary, consider whether the Government's assertion of the law enforcement privilege with respect to certain discovery would apply to outweigh Mr. Jean's need for the evidence.

On October 19, 2016, the Court issued a text-only Order, explaining that it required further development of the record as to the Government's assertion of the law enforcement privilege. The Court then directed the Government to prepare and submit for *in camera* review a confidential brief, supported by affidavits and any other evidence the Government deemed relevant, on the subject of the privilege. In a separate email to the parties, the Court advised Mr. Jean's counsel that he was welcome to submit a supplemental brief on the law enforcement privilege, if he so desired. On November 19, 2016, the Court received

and reviewed a confidential and classified affidavit from the Government setting forth a factual basis in support of its assertion of the law enforcement privilege, and also received and reviewed Mr. Jean's Supplementary Brief on the privilege (Doc. 46).

The Court now finds that the above issues are ripe for decision. For the reasons explained herein, the Court **GRANTS IN PART AND DENIES IN PART** the Motion to Compel (Doc. 28).

I. BACKGROUND

The Court previously set forth a detailed recitation of the background facts surrounding this case in its Memorandum Opinion and Order on Mr. Jean's Motion to Suppress. *See* Doc. 40. The Court therefore incorporates those background facts by reference, and highlights below a few salient details about the case to provide context for the Court's rulings.

Mr. Jean's arrest and indictment proceeded from the FBI's development of specialized electronic investigative technology that was intended to identify the registered users of a child pornography website known as "Playpen." Playpen operated as a hidden service on the TOR network. This network could be accessed by anyone who downloaded the TOR browser, which in turn allowed users to mask their true Internet Protocol ("IP") addresses so that they could search the web in complete anonymity. Because the Playpen website was located on the TOR network, and users of the website had masked their true IP addresses, law enforcement lacked the means to identify those individuals who were actively downloading and distributing child pornography on Playpen. The FBI developed certain computer code, which it dubbed a "Network Investigative Technique" ("NIT"), that

would surreptitiously deploy when a Playpen user would log into the website using a username and password, and begin downloading an image of child pornography. The NIT would then cause the user's computer to send back to the FBI certain content-neutral identifying information, including the computer's type of operating system, the computer's host name and operating system username, the computer's media access control address, and a unique identifier generated by the NIT. The user's return of this "packet" of information was sent to the Government's computer over the regular internet—which had the intended side effect of revealing the user's true IP address, because IP addresses are attached to every packet of information exchanged over the regular internet. With the user's true IP address came the FBI's ability to determine the actual identity and location of the suspected Playpen user. The FBI's NIT was able to do all this by first exploiting a defective window, *i.e.*, a non-publicly-known vulnerability, [redacted].

Mr. Jean agrees the Government already provided certain NIT related information in discovery. First, the Government provided the operating instructions that were sent to Mr. Jean's computer at the time he allegedly began downloading child pornography from the Playpen website. During the hearing, the parties and their witnesses sometimes referred to these operating instructions as the "payload," whereas at other times, they referred to the instructions as "the NIT." Second, the Government produced the raw data that was received by the FBI from Mr. Jean's computer and internet modem. This data was also referred to during the hearing as the "two-way data stream" between the FBI's computer and Mr. Jean's computer, or the "PCAP data." Third, the Government disclosed the particular images that were downloaded by a Playpen user called "regalbegal"—whom the Government contends is Mr. Jean. Fourth, the Government made available the

contents of Mr. Jean's seized computer, which the Government asserts contains contraband evidence of child pornography that was seized pursuant to the residential search warrant executed at Mr. Jean's residence.

Although acknowledging the production of all this evidence, Mr. Jean argues there are still other pieces of evidence in the Government's possession that are material to Mr. Jean's defense and should be provided in discovery. The first piece of evidence is the computer code that the FBI used to generate the "unique identifier" that was used to link Mr. Jean's computer to the user who accessed and downloaded images from the Playpen website with the regalbegal username. This unique identifier is an algorithm, or sequence of numbers, that the FBI created and later associated with regalbegal's Playpen account. During the hearing on the Motion to Compel, the Court asked whether the Government would consider voluntarily providing the unique-identifier code to Mr. Jean's expert, Dr. Miller, subject to a protective order drafted by the parties and submitted to the Court for approval. The Government agreed to this compromise, and an agreed protective order concerning this production was entered under seal. *See* Doc. 43. Accordingly, the Court **GRANTS IN PART** the Motion to Compel as to Mr. Jean's request for the unique-identifier code, subject to the protective order, which limits disclosure of this information to Dr. Miller and Mr. Jean's current attorneys of record who are employed by the Office of the Federal Public Defender.

Next, Mr. Jean requests the NIT, or "payload" data, in a more readable source-code format, rather than the assembly-code format that the Government provided.[1] Agent Alfin

[1] Dr. Miller testified during the hearing that computer code is most often written in "source-code" format, which is a descriptive term for code that is written in a programming

testified during the hearing that the NIT code was never written in source-code language, but was instead written directly in assembly-code language. Upon questioning by the Court at the conclusion of the hearing, Mr. Jean's counsel confirmed that he was now satisfied that this particular issue had been resolved, in light of Agent Alfin's testimony. *See* Doc. 44, p. 109. Accordingly, the Court **FINDS AS MOOT** Mr. Jean's request for a source-code version of the NIT instructions.

Mr. Jean's third and final request[2] is for the Government to disclose the source code for the "exploit," a piece of software that the Government used to electronically bypass TOR's encryption safeguards. Mr. Jean argues that having the code for the exploit

---

language that is easier for a human to read. Code may also be written in "assembly-code language," which Agent Alfin explained is a low-level programming language similar to binary code and is not user-friendly.

[2] Mr. Jean's briefing originally included a fourth request for all the data that the FBI received from regalbegal and logged on its server after the NIT deployed. Dr. Miller testified that if the defense had access to this information, which he referred to as the "server component," the defense could better understand how the FBI recorded both regalbegal's unique identifier and the two-way data stream resulting from the NIT. By analyzing the server, the defense could verify whether the FBI logged all this data correctly, or else duplicated the data or made some other coding error. Agent Alfin testified that the Government already provided the defense with both the raw network data that was produced by the NIT—before the data even hit the FBI's server—as well as the data generated by the server after the fact. Since the raw data exactly matched the server data, this indicated to Agent Alfin that the server accurately logged and reproduced all the data it received. Following this testimony, the Court was prepared to rule that the server component was not material to the defense; however, Mr. Jean's counsel, Mr. Alfaro, dropped the argument when the Court questioned him at the end of the hearing as to which pieces of information he still requested. ("COURT: So we're down to two things, two categorical pieces of information. One is what I have described as the exploit code and the second being the source code that would be associated with how the unique identifying numbers are generated. Those are the two things that you're after at this point that you don't have. MR. ALFARO: That's correct, Judge."). (Doc. 44, pp. 109-110). Accordingly, the Court finds that the request for the server component was abandoned by the defense and is therefore **MOOT**.

would allow him to understand the means and methods by which the FBI was able to take advantage of a vulnerability [redacted] which in turn allowed the NIT's instructions to be executed on Mr. Jean's computer. In layman's terms, the TOR browser's encryption and anonymity features can be analogized to a lock, and the exploit software to a lock-pick.

The Government refuses to surrender the exploit code for two reasons. First, it argues the exploit code is not material to the defense under Federal Rule of Criminal Procedure 16(a)(1)(E)(i). According to the Government, discovery of the exploit code, *i.e.*, knowing *how* the lock was picked, is not relevant or useful to understanding how the NIT code obtained identifying information from Mr. Jean's computer, nor would such knowledge assist or diminish a defense based on third-party hacking. Second, the Government argues that even if the exploit code were found to be material, it should not be disclosed because such disclosure would be subject to the qualified law enforcement privilege and would compromise the integrity of the FBI's investigatory and surveillance functions with respect to similar investigations.

Mr. Jean believes the exploit code is material because there exists the possibility that his computer may have suffered some unintended change or other consequence as a result of the FBI running the exploit. In particular, Mr. Jean suggests that the exploit may have disabled the firewall on his computer or inserted a certificate into the TOR browser that could have left the computer vulnerable to outside attacks by third parties. In Mr. Jean's view, a third-party attack could potentially explain why child pornography was present on his computer at the time it was seized. Below, the Court will recite the appropriate legal standard that governs this dispute, and then consider Mr. Jean's

arguments in favor of disclosure of the exploit code, balanced against the Government's arguments against disclosure.

II. LEGAL STANDARD

Rule 16(a)(1)(E) provides:

> Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:
>
> (i) the item is material to preparing the defense;
>
> (ii) the government intends to use the item in its case-in-chief at trial; or
>
> (iii) the item was obtained from or belongs to the defendant.

Information is considered "material" if it is "helpful to the defense." *United States v. Vue*, 13 F.3d 1206, 1208 (8th Cir. 1994). In the absence of more detailed guidance from the Eighth Circuit on what the term "material" means, this Court agrees with the reasoning of the District Court of the District of Columbia that "the government cannot take a narrow reading of the term 'material' in making its decisions on what to disclose under Rule 16. Nor may it put itself in the shoes of defense counsel in attempting to predict the nature of what the defense may be or what may be material to its preparation." *United States v. Safavian*, 233 F.R.D. 12, 15 (D.D.C. 2005).

The materiality hurdle is not intended to be a high one. In fact, even inculpatory evidence, once disclosed by the government, "is just as likely to assist in 'the preparation of the defendant's defense' as exculpatory evidence." *United States v. Marshall*, 132 F.3d 63, 67 (D.C. Cir. 1998). By the same token, the defendant's burden of proof as to

materiality must meet some minimal standard. "A showing of materiality . . . , is not satisfied by a mere conclusory allegation that the requested information is material to the preparation of the defense." *United States v. Krauth*, 769 F.2d 473, 476 (8th Cir. 1985) (internal quotation and citation omitted). Instead, the defendant "must demonstrate that the requested evidence bears some abstract logical relationship to the issues in the case." *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993) (internal quotation and citations omitted).

When the Government asserts the qualified law enforcement privilege to justify withholding certain information that the defense claims is material, the Court must "weigh all relevant factors, including the crime charged, potential defenses, and the possible significance of the [privileged information]" to determine whether the defendant's need for the information outweighs the interests of the public in keeping the information secret. *See Barnes v. Dormire*, 251 F.3d 767, 770 (8th Cir. 2001). In the Supreme Court case of *Roviaro v. United States*, 353 U.S. 53, 60-61 (1957), the government refused to reveal to the defendant the identity of a confidential informant who was involved in a drug transaction that resulted in the defendant's conviction. The Court explained that where the disclosure of privileged information "is essential to a fair determination of a cause, the privilege must give way. In these situations the trial court may require disclosure and, if the Government withholds the information, dismiss the action." *Id.* Making a decision about whether to compel the government to disclose information "calls for balancing the public interest in protecting the flow of information against the individual's right to prepare his defense." *Id.* at 62. Therefore, the particular circumstances of the case must be examined

by the court, focusing on "the crime charged, the possible defenses, the possible significance of the [privileged information], and other relevant factors." *Id.*

Further guidance is found in the Fifth Circuit case of *In re United States Department of Homeland Security*, 459 F.3d 565 (5th Cir. 2006). In that case, the government sought to invoke the law enforcement privilege to protect the production of certain documents. The Court first explained that it is the obligation of the district court to "review the documents at issue *in camera* to evaluate whether the law enforcement privilege applies," and next to "balance 'the government's interest in confidentiality against the litigant's need for the documents.'" *Id.* at 570 (quoting *Coughlin v. Lee*, 946 F.2d 1152, 1160 (5th Cir. 1991)). The Court also noted that the law enforcement privilege is "qualified," in that it is "bounded by relevance and time constraints." *Id.* at 571.

III. DISCUSSION

As the parties have resolved two of the issues raised in the Motion to Compel, only one issue remains: whether the Government should be required to surrender the computer code for the exploit. Mr. Jean argues that the exploit code is material to his defense. The Government argues that the exploit code is not material to his defense; but even if it were considered material in some respect, discovery is nevertheless protected by the qualified law enforcement privilege. In deciding whether the Government should be compelled to produce the exploit code, the Court must then balance the public interest in keeping the exploit code secret against Mr. Jean's need for the code to prepare his defense. The particular facts in this case will drive the analysis.

A. Materiality

First, the Court will take up the issue of the materiality of the exploit code to Mr. Jean's defense. In support of that argument, Mr. Jean submits the Declarations of Vlad Tsyrklevich (Doc. 28-1), Robert Young (Doc. 28-2), and Shawn Kasal (Doc. 28-4), all computer experts who were retained by defendant Jay Michaud in a related Playpen/NIT case currently proceeding in the Western District of Washington. *See United States v. Michaud*, No. 3:15-CR-05351 (W.D. Wash.). These three declarants opined in the context of the *Michaud* case that possessing *all the code* related to the FBI's Playpen investigation would be material to Mr. Michaud's defense. Mr. Tsyrklevick also opined that possessing the exploit code in particular would be critical to verifying "whether the exploit executed additional functions outside the scope of the NIT warrant." (Doc. 28-1, p. 3). The Court has now reviewed these declarations and finds them generally unpersuasive, as they were prepared in the context of another case and fail to shed light on the particular facts and circumstances surrounding Mr. Jean's case. Also, the declarants' opinions were not subject to cross-examination by counsel for the Government.

With respect to defense witness Dr. Miller, however, the Court places substantial weight upon his opinion, as he not only submitted a declaration in *Michaud* (Doc. 28-3), but also appeared via videoconference at the hearing on Mr. Jean's Motion to Compel. Dr. Miller was subjected to cross-examination by the Government, and his opinions were tailored to the facts of this case. The Court similarly places substantial weight on the

testimony of Agent Alfin,[3] who appeared in person at the hearing and was subjected to cross-examination by counsel for Mr. Jean.

Dr. Miller testified that if he were permitted to examine the exploit code, he could determine exactly what the exploit did to penetrate the presently unknown vulnerability in [redacted] and in doing so, verify that the exploit only "picked the lock" on Mr. Jean's [redacted], and did not also make other changes to his computer that could have subjected it to a third-party attack. When Dr. Miller was pressed to explain exactly how a third party could have used the exploit to attack or hack into Mr. Jean's computer, Dr. Miller reasoned that since the FBI sent a copy of the exploit to all Playpen users in the course of the sting operation, any of these users could have potentially identified the exploit and "leveraged that [exploit] to do whatever they wanted." (Doc. 44, p. 55). He conceded that the likelihood of a user both identifying the exploit and using it to hack another user's computer was vanishingly small. A hacker such as this would have been both sophisticated in his computer skills and very proactive in using them; would have believed that the FBI was actively monitoring him at the same time he was accessing the Playpen website; would have understood exactly how an exploit works and, in Dr. Miller's terms, how to "capture data streams" and "get the exploit out," *id.*; would have been constantly monitoring the Playpen website for subtle code changes that could indicate when the exploit was deployed, *id.* at pp. 58-59; and would have been trying to "catch" the exploit

---

[3] The Government submitted an additional declaration from Supervisory Special Agent [redacted] (Doc. 30-5), who did not appear at the hearing but only submitted his declaration in the context of the *Michaud* case. For the same reasons previously explained, the Court gives little consideration to Agent [redacted] declaration, as it was not submitted in the context of the case at bar, and he was not subjected to cross-examination by Mr. Jean's counsel.

code as it was deployed—even though exploits were sent to users' computers over an encrypted network, and the time it took to send the NIT and receive identifying information for a user was less than a third of a second.

Dr. Miller initially opined that the plausibility of a third party using the exploit to successfully hack into another Playpen user's computer was slightly above the "very unlikely" point, on a scale of "likely" to "very unlikely." *See id.* at p. 58. Later on in his testimony, however, Dr. Miller revised his opinion after learning on cross-examination (or being asked to assume) that Mr. Jean admitted to investigators that he was, in fact, the Playpen user known as regalbegal, and also that he had downloaded child pornography from the Playpen website.[4] Assuming those case-specific facts, Dr. Miller acknowledged that the possibility of third-party hacking in Mr. Jean's particular case was "much less likely" than he had previously opined. *Id.* at p. 60.

When Agent Alfin took the stand, he agreed with Dr. Miller that very few individuals would be capable of successfully taking advantage of an exploit to hack into a fellow Playpen user's computer. According to Agent Alfin, a hacker such as this would have had to have known in advance that the FBI was conducting a sting operation, and would have installed certain software on his computer to intercept traffic going into and out of the TOR proxy. Further, in Agent Alfin's view, in order to capture the exploit when the FBI deployed it, the hacker would have had "to be monitoring traffic on their local computer, going to and from the TOR proxy on their computer," *id.* at p. 84, and analyzing "a massive amount of data" to eventually find the exploit and then "reuse it for their own purposes," *id.* at pp. 84-

[4] Mr. Jean has not contested the Government's representations that Mr. Jean made such admissions to law enforcement during and after execution of a residential search warrant.

85. The likelihood of doing all this during the brief 13-day window in which the FBI controlled the Playpen server was, in Agent Alfin's estimation, "zero" or "[w]hatever tiny number is slightly higher than zero," and was "a farfetched theoretical possibility." *Id.*

Agent Alfin also pointed out that no defense expert had bothered to examine Mr. Jean's computer to determine whether the exploit did, in fact, disable a firewall or make either a temporary or permanent change to the operating system that could have been detected. By contrast, Agent Alfin personally executed the NIT on a computer running an operating system configured to mimic Mr. Jean's computer. While running this experiment, Agent Alfin noted that his computer's security firewall was not disabled by the exploit, nor were any security settings or default configurations affected. *See id.* at pp. 92-93. He also examined whether any of the active ports that allowed his computer to communicate with others had changed in some way, and he testified that the ports remained the same. *Id.* at p. 93. Although counsel for Mr. Jean pointed out on cross-examination that Agent Alfin did not review every single file on his computer for possible changes caused by the exploit, the Court finds persuasive the fact that Agent Alfin tested the NIT on an exemplar computer and made observations; whereas Mr. Jean's experts failed to run any tests on Mr. Jean's computer, despite the fact that they had access to it.

In considering Mr. Jean's Motion to Compel, the Court is mindful of the relatively low bar he must meet under Rule 16(a)(1)(E) to entitle him to the disclosure of information under the Government's control. Nonetheless, a defendant may not rest his entire argument in support of compelling discovery on a virtually impossible hypothetical situation. This is particularly true here, where the stated material need was further undermined by Agent Alfin's un-rebutted testimony as to his testing of the defense hypothetical on an

exemplar computer. Ultimately, Mr. Jean's argument is simply that his expert might, perhaps, be able to make something of the exploit code if he knew how it works. The Court finds this argument untenable, because simply knowing how the exploit picked the lock would not materially assist the defense in better understanding the relative plausibility of a third-party hacking defense. Regardless of what Dr. Miller might learn from the exploit code, the third-party hacker defense would still be predicated on the simultaneous existence of a long string of hypothetical circumstances. Mr. Jean's argument fails to "demonstrate that the requested evidence bears some abstract logical relationship to the issues in the case." *Lloyd*, 992 F.2d at 351. For these reasons, the Court finds as a threshold matter that Mr. Jean has failed to establish that discovery of the exploit code would be material to his defense. This determination, in and of itself, should warrant denial of the Motion to Compel as to the exploit.

B. Qualified Law Enforcement Privilege

Giving Mr. Jean the benefit of the doubt, however, and assuming hypothetically that his showing of materiality, while negligible, is just strong enough to warrant engaging in a balancing test, the Court finds that any need for the exploit that Mr. Jean has demonstrated is greatly outweighed by the public's interest in keeping the exploit secret. The Court reviewed *in camera* a confidential affidavit submitted by the Government, [redacted]

[redacted]. The public interest is therefore well served by keeping the exploit code secret.

The Court further finds that permitting Mr. Jean, his computer expert, and his defense attorneys to examine the exploit under a classified protective order would not effectively address the Court's confidentiality concerns, [redacted] The risk that the information might inadvertently be leaked or otherwise used by third parties is too great, and outweighs any argument Mr. Jean has made in favor of obtaining the exploit code for his defense. Even if Mr. Jean's expert, and no one else, were shown the exploit code, the knowledge gained by the expert as to the nature of the code and how the exploit works could not be erased from his memory. Protective orders have limitations. Mere knowledge of the particular vulnerability exploited here could potentially lead the expert to later build his own exploit, or assist others in doing so, thereby effectively circumventing a protective order. The public should not bear this risk.

IV. CONCLUSION

IT IS THEREFORE ORDERED that Defendant Anthony Allen Jean's Motion to Compel (Doc. 28) is **GRANTED IN PART AND DENIED IN PART** as follows: (1) Mr. Jean's request for the unique-identifier code is **GRANTED**, but subject to a protective order; (2) Mr. Jean's request for the source code for the NIT or "payload" data is **MOOT**; and (3) Mr. Jean's request for the exploit code is **DENIED**.

The Clerk is **ORDERED** to file this Opinion and Order under seal, with access granted only to court users and the attorneys of record.

IT IS SO ORDERED on this 16th day of November, 2016.

TIMOTHY L. BROOKS
UNITED STATES DISTRICT JUDGE